AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter, where the underlining ("___") indicates the language being added and strikethrough ("——") indicates the language being deleted, as is applicable.

Listing of Claims:

1-28. (Canceled)

29. (Currently Amended) An email filtering system comprising:

an electronic messaging client for viewing electronic messages addressed to a user, the electronic messaging client having a single graphical user interface control to provide, to the user, options for configuring each of a plurality of detection mechanisms that detect undesired electronic messages from incoming electronic messages retrieved for the user, the single graphical user interface control enabling the user to activate and deactivate each of the plurality of detection mechanisms independently of one another in order to provide a desired level of protection from undesired electronic messages, wherein the plurality of detection mechanisms comprise at least three different detection mechanisms used to detect undesired electronic messages, wherein the plurality of detection mechanisms include:

a first detection mechanism that detects an email message if the sender of the email message is not on a list of senders authorized by the user;

a second detection mechanism that detects an email message if the sender of the email is on a list of unauthorized senders;

a third detection mechanism that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content string; and

a fourth detection mechanism that is configured to:

analyze the overall content of previous email messages that have been detected;

compare the content of an email message to the overall content and assign a score reflective of a level of similarity for the email message; and

detect the email message if the score is higher than a designated score.

30-34. (Canceled)

35. (Currently Amended) The system of claim ~~34~~ 29, wherein the single graphical interface comprises:

a first interface mechanism to activate the first detection mechanism;

a second interface mechanism to activate an interface to edit the list of senders authorized by the user;

a third interface mechanism to activate the second detection mechanism;

a fourth interface mechanism to activate an interface to edit the list of senders not authorized by the user;

a fifth interface mechanism to activate the third detection mechanism;

a sixth interface mechanism to activate an interface to edit the list of unauthorized textual content strings;

a seventh interface mechanism to activate the fourth detection mechanism, and

an eighth interface mechanism to adjust the designated score.

36. (Previously Presented) The system of claim 35, wherein the interface to edit the list of unauthorized textual content strings is configured to display a list of the detected textual content strings in particular undesired email message that was detected by the third detection mechanism, the interface to edit the list of unauthorized textual content strings further configured to substitute different textual strings for the detected textual content strings.

37. (Previously Presented) The system of claim 35, wherein the interface to edit the list of unauthorized textual content strings is configured to display a particular undesired email message with the detected textual content strings in the particular undesired email message highlighted so that the user may select a particular highlighted detected textual content string, the interface to edit the list of unauthorized textual content strings being configured to remove the particular highlighted detected textual content string from the unauthorized list of textual content strings.

38. (Currently Amended) The system of claim ~~34~~ 29, wherein the email client displays a particular undesired email message in a particular manner that is representative of the particular detection mechanism that detected the particular undesired email message.

39. (Previously Presented) A method for providing electronic messaging, comprising:

providing a plurality of detection approaches for detecting undesired email messages; and

providing access to each of the detection approaches from a single graphical interface control, the single graphical user interface control enabling the user to activate and deactivate each of the plurality of detection mechanisms independently of one another in order to provide a desired level of protection from undesired electronic messages, wherein the plurality of detection mechanisms comprise at least three different detection mechanisms used to detect undesired electronic messages.

40. (Previously Presented) The method of claim 39, wherein the plurality of detection approaches include an approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user.

41. (Previously Presented) The method of claim 39, wherein the plurality of detection approaches include an approach that detects an email message if the sender of the email is on a list of unauthorized senders.

42. (Previously Presented) The method of claim 39, wherein the plurality of detection approaches include an approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content strings.

43. (Previously Presented) The method of claim 39, wherein the plurality of detection approaches include an approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of the previous messages.

44. (Previously Presented) The method of claim 39, wherein the plurality of detection approaches include:

a first approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user;

a second approach that detects an email message if the sender of the email is on a list of unauthorized senders;

a third approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content string; and

a fourth approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of previous messages according to a designated content score.

45. (Currently Amended) The method of claim ~~45~~ 44, further comprising:

from the single graphical interface control, activating the first detection approach;

from the single graphical interface control, activating an interface for editing the list of senders authorized by the user;

from the single graphical interface control, activating the second detection approach;

from the single graphical interface control, activating an interface to edit the list of senders not authorized by the user;

from the single graphical interface control, activating the third detection approach;

from the single graphical interface control, activating an interface for editing the list of unauthorized textual content strings;

from the single graphical interface control, activating the fourth detection mechanism, and

from the single graphical interface control, adjusting the designated content score.

46. (Currently Amended) The method of claim ~~46~~ 45, wherein the interface to edit the list of unauthorized textual content strings is configured to display a list of the detected textual content strings in particular undesired email message that was detected by the third approach, the interface to edit the list of unauthorized textual content strings further configured to substitute different textual strings for the detected textual content strings.

47. (Previously Presented) The method of claim 46, wherein the interface to edit the list of unauthorized textual content strings is configured to display a particular undesired email message that was detected by the third approach with the detected textual content strings in the particular undesired email message highlighted so that the user may select a particular highlighted detected textual content string, the interface to edit the list of unauthorized textual content strings being configured to remove the particular highlighted detected textual content string from the unauthorized list of textual content strings.

48. (Previously Presented) The method of claim 39, further comprising:

displaying a particular undesired email message in a particular manner that is representative of the particular detection approach that detected the particular undesired email message.

49. (Currently Amended) A computer readable medium ~~having a~~ comprising a tangible medium embodied with an embedded computer program for providing electronic messaging, the program when executed by a computer causes the computer to perform:

providing a plurality of detection approaches for detecting undesired email messages; and

providing access to each of the detection approaches from a single graphical interface control, the single graphical user interface control enabling the user to activate and deactivate each of the plurality of detection mechanisms independently of one another in order to provide a desired level of protection from undesired electronic messages, wherein the plurality of detection mechanisms comprise at least three different detection mechanisms used to detect undesired electronic messages.

50. (Previously Presented) The computer readable medium of claim 49, wherein the plurality of detection approaches include an approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user.

51. (Previously Presented) The computer readable medium of claim 49, wherein the plurality of detection approaches include an approach that detects an email message if the sender of the email is on a list of unauthorized senders.

52. (Previously Presented) The computer readable medium of claim 49, wherein the plurality of detection approaches include an approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content strings.

53. (Previously Presented) The computer readable medium of claim 49, wherein the plurality of detection approaches include an approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of the previous messages.

54. (Previously Presented) The computer readable medium of claim 49, wherein the plurality of detection approaches include:

a first approach that detects an email message if the sender of the email message is not on a list of senders authorized by the user;

a second approach that detects an email message if the sender of the email is on a list of unauthorized senders;

a third approach that detects an email message if the email message contains a textual content string that is on a list of unauthorized textual content string; and

a fourth approach that analyzes the overall content of previous email messages that have been detected and detects an email message if the content of the message is similar to the overall content of previous messages according to a designated content score.

55. (Previously Presented) The computer readable medium of claim 54, the program further comprising:

from the single graphical interface control, activating the first detection approach;

from the single graphical interface control, activating an interface for editing the list of senders authorized by the user;

from the single graphical interface control, activating the second detection approach;

from the single graphical interface control, activating an interface to edit the list of senders not authorized by the user;

from the single graphical interface control, activating the third detection approach;

from the single graphical interface control, activating an interface for editing the list of unauthorized textual content strings;

from the single graphical interface control, activating the fourth detection mechanism, and

from the single graphical interface control, adjusting the designated content score.

56. (Previously Presented) The computer readable medium of claim 55, wherein the interface to edit the list of unauthorized textual content strings is configured to display a list of the detected textual content strings in particular undesired email message that was detected by the third approach, the interface to edit the list of unauthorized textual content strings further configured to substitute different textual strings for the detected textual content strings.

57. (Previously Presented) The computer readable medium of claim 55, wherein the interface to edit the list of unauthorized textual content strings is configured to display a particular undesired email message that was detected by the third approach with the detected textual content strings in the particular undesired email message highlighted so that the user may select a particular highlighted detected textual content string, the interface to edit the list of unauthorized textual content strings being configured to remove the particular highlighted detected textual content string from the unauthorized list of textual content strings.

58. (Previously Presented) The computer readable medium of claim 49, further comprising:

displaying a particular undesired email message in a particular manner that is representative of the particular detection approach that detected the particular undesired email message.